REMARKS

Applicants would like to thank the Examiners Reagan and Hayes for the courtesies extended during the personal interview of December 10, 2002. The following will summarize the discussion during the interview, in a slightly more expanded manner than the Examiner's Interview Summary form, pursuant to the Examiner's oral request.

The Office Action of October 4, 2002 includes a rejection of claims 1-6 and 15-17 under 35 U.S.C. §103 as allegedly being unpatentable over the *Reed et al.* patent (U.S. Patent No. 5,862,325) in view of the *Pistriotto et al.* patent (U.S. Patent No. 6,138,162) and rejection of claims 7-14 under 35 U.S.C. §103 as allegedly being unpatentable over the combination of the *Reed et al.* and *Pistriotto et al.* patents and further in view of the *Papierniak et al.* patent (U.S. Patent No. 6,128,624). These rejections were respectfully traversed during the interview for the following reasons.

As discussed in the background section of the present application, there are several protocols used in collecting data about consumers' buying habits. With respect to the Internet, Internet-activity monitoring has been proposed. For example, a server-side consumer data collection strategy has been proposed in which an individual Internet content provider or website monitor and collects data about each consumer who has requested data from the visited website and compiles this data about all consumers who have visited that particular website. Alternatively, the website could actually collect data from the individual about his or her buying habits, e.g., by way of on-line surveys, for which compensation is given.

As a different alternative, data collection directly from the Internet consumers' computers has also been proposed. This is known as client-side data collection. However, client-side data collection involves installing large and cumbersome software applications on the consumers' computers, which operates at the same time as an Internet browser application software. Internet activity data is then collected and presumably also filtered and thereafter uploaded to a data collecting computer on the Internet. There are disadvantages of such a system including consumption of computer power of the PC, and consumption of bandwidth of the Internet connection, not to mention the difficulty in upgrading or updating the distributed application software on the consumers' computers.

The present invention involves a method of collecting data relating to a user's transactions over an unsecure network. The user utilizes a computing device to send and receive data sets over the network wherein the computing device has an address on the network. The data sets include data representative of the address of the computing device on the network.

In contrast to the applied art, the method of the present invention also includes the step of directing all data sets through a computing device to a known domain. Hence, all data coming from the computing device is forwarded directly to a known domain, rather than directly to any of the URLs or other domains on the Internet as is typically done. In an exemplary embodiment, the user actually agrees to allow his or her browser software to be modified to direct all data sets from the computing device to the known domain of the service provider.

Additionally, the present invention assigns a unique identifier to the computing device, which is separate and apart from the computing device's address on the network. This unique identifier differentiates the computing device from other computers that similarly direct data sets from computing devices to send known domain.[1] Applicants respectfully submit that nothing in the applied prior art teaches or suggests this aspect of the present invention, particularly when taken in combination with the other recitations as discussed herein.

The present invention, as recited in claim 1, readdresses the data sets from the computing device to indicate that the data sets originated from the known domain.

Further, the present invention records at least part of the data sets, which may include data other than the computing device's address on the network, such as product ordering information, etc. The readdressed data is sent onto the network. Claim 1 recites each of these aspects of the present invention.

It is noted that the three steps of directing all the data sets from the computing device to a known domain, assigning a unique identifier to the computing device and recording at least part of the data sets with respect to the unique identifier, in combination with the other recitations of claim 1, present novel aspects of the present invention.

---

[1] The newly added language to the claim is somewhat different from the language proposed during the Interview. It has direct support in the original specification at page 16, lines 7-12.

The *Reed et al.* Patent

The *Reed et al.* patent includes a broad discussion of computer base communication systems, and a discussion of a way to coordinate the transfer of data, meta data and instructions between databases in order to control and process communications. In relevant part, as cited by the Examiner, the *Reed et al.* patent discloses an HTTP redirect command. A HTTP redirect is a URL that is automatically processed by the web software that made the original URL request. In this way, a host can "resolve" a first URL into a second URL. In this manner, a succession of redirects is possible until the final resource is resolved, as discussed at column 80, lines 38 *et seq.*

The *Pistriotto et al.* Patent

The *Pistriotto et al.* patent in relevant part as cited by the Examiner discloses a proxy gateway server in column 3. This patent provides an explanation of the different types of proxy servers used on the Internet in columns 2 and 3. In the portion cited by the Examiner, a request URI can be processed under one of three options. For instance, the request URI does not apply to a particular resource, but to the server itself, is only allowed when the method does not necessarily apply to the resource. The second or absolute URI form is required when the request is being made to a proxy, wherein the proxy is requested to forward the request or service it from a valid cache, and return the response. The third involves the URI being transmitted from a resource in the original service or a gateway is identified. It is respectfully submitted that these aspects of the *Pistriotto et al.* patent does not disclose, teach or suggest the present recitations of claim 1, whether read alone or in

combination with the *Reed et al.* patent. Specifically, in combination, the two references do not teach or suggest *inter alia* directing all data sets for a computing device to a known domain, assigning a unique identifier to the computing device and recording at least part of the data sets, as indicated in the context of claim 1.

Further, independent claim 16 includes similar recitations to those relied upon above and therefore claim 16 is patentable for at least the same reasons that independent claim 1 is patentable.

With respect to newly made independent claim 5 and claim 17, it is respectfully noted that the applied art does not teach or suggest negotiating a first encryption key with a computing device and negotiating a second encryption key with intended recipient of the data sets sent by a computing device. This aspect of the present invention is important insofar as in an exemplary embodiment, a domain in accordance with the present invention is interposed between the client or user's computing device and the website that the client is requesting. An intercepted encrypted message is decoded, then re-encoded and forwarded on to the requested URI, for example. In this way, otherwise secured transaction details can be gathered, with the user's permission, for example. This is done by encryption key protocols wherein a first encryption key is negotiated with a computing device, and a second encryption key is negotiated with the intended recipient of the data sent by the computing device. There is no indication in the applied art of any appreciation of this mechanism.

Hence, claim 5 has been placed in independent form to emphasize this aspect of the present invention, and it is respectfully submitted that claims 5, 6 and 17 are also separately patentable.

Other dependent claims were not been discussed for sake of brevity during the interview, nor was the *Papierniak et al.* patent discussed in great detail. Applicants note in passing that the *Papierniak et al.* patent appears to indicate the data is collected at the server at column 14, lines 19-22, in its discussion of the web tracking module 300. See also column 15 lines 58 *et seq.* where various types of information are identified as well as the discussion in column 15, lines 29-37, regarding web logs at various points.

At the conclusion of the interview, it appeared to the undersigned that the Examiner would conduct a further search in light of these comments but appeared to be inclined to at least withdraw or modify the present rejections and perhaps allow the application in light of the discussion during the interview.

Applicants respectfully request reconsideration and allowance of the present application. Should any residual issues exist, the Examiner is invited to contact the undersigned at the number listed below.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: January 3, 2003

Attachment to Amendment dated January 3, 2003

Marked-up Claims 1, 5 and 16

1. A method of collecting data relating to a user's transactions over an unsecure network, the user utilizing a computing device to send and receive data sets over the network, the computing device having an address on the network, the data sets including data representative of the address of the computing device on the network, comprising the steps of:

directing all data sets from the computing device to a known domain;

assigning a unique identifier to the computing device to differentiate it from other computers that similarly direct data sets from computing devices to said known domain;

readdressing data sets sent from the computing device to indicate that the data sets originated in the known domain;

recording at least part of the data sets; and

sending the readdressed data onto the network.

5. A method of collecting data relating to a user's transactions over an unsecure network, the user utilizing a computing device to send and receive data sets over the network, the computing device having an address on the network, the data sets including data representative of the address of the computing device on the network, comprising the steps of:

Attachment to Amendment dated January 3, 2003

Marked-up Claims 1, 5 and 16

directing all data sets from the computing device to a known domain;

assigning a unique identifier to the computing device;

readdressing data sets sent from the computing device to indicate that the data sets originated in the known domain;

recording at least part of the data sets;

sending the readdressed data onto the network; [A method according to Claim 1, further comprising the steps of:]

negotiating a first encryption key with the computing device; and

negotiating a second encryption key with an intended recipient of a data set sent by the computing device.

16. A system for collecting data relating to a user's transactions over an unsecure network, the user using a computing device configured to send and receive data sets over the network, the computing device having an address on the network, the data sets including data representative of the address of the computing device on the network, the system comprising:

logic configured to assign a unique identifier to the computing device to differentiate it from other computers that similarly direct data sets from computing devices to said known domain;

logic configured to readdress data sets sent from the computing device

Attachment to Amendment dated January 3, 2003

Marked-up Claims 1, 5 and 16

to indicate that the data sets originated in the known domain;

logic configured to record at least part of the data sets; and

logic configured to send the readdressed data onto the network.